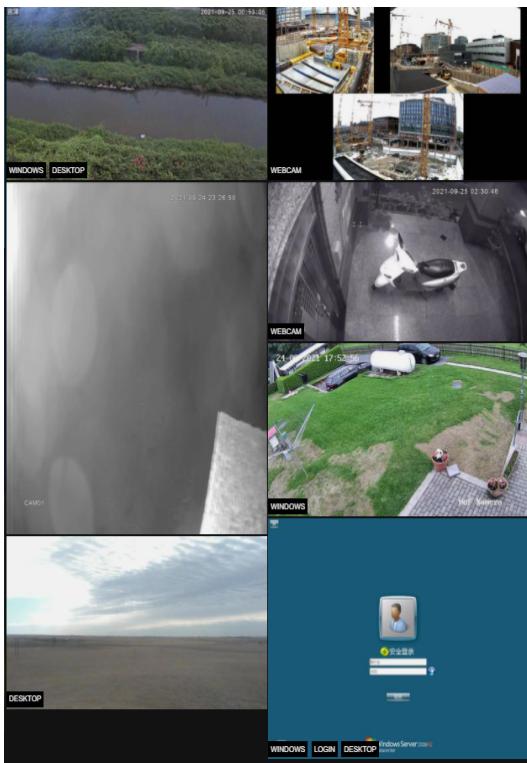


# Lab 5

## Exploring Shodan



**Estimated time to complete: 20 Min**

### WHAT YOU WILL LEARN

Shodan is a search engine for Internet-connected devices. Search for open ports or abuse default passwords to discover everything from web cams, power plants, cell phones, refrigerators, and Minecraft servers.

Let's go exploring and see what we can find!

### WHY IT'S IMPORTANT

Explore and understand the dangers that come with a lack of security with devices connected to the open network

Understand the basics of port scanning across the entire internet and how attackers can find your device even without it being connected to a domain name

### SKILLS GAINED

- Port scanning
- Open Source Intelligence
- Understanding of “Open Internet”
- How to view open devices

### REQUIRED HARDWARE

- Raspberry Pi
- Internet connection

**DISCLAIMER: THIS LAB WILL SHOW YOU HOW TO VIEW THESE PUBLIC DEVICES. HOWEVER, TRYING TO ACCESS OR CONTROL THESE DEVICES IS ILLEGAL. USING SHODAN IS LEGAL, ACCESSING SOMEONE ELSE'S DEVICE IS NOT! DO NOT ATTEMPT TO USE OR MODIFY THE DEVICES FOUND.**

## INTRODUCTION TO SHODAN



Shodan is a search engine for cyber security individuals. Unlike Google, Shodan allows its users to search for devices that are open to the public internet and filter those results based on the user's wants. It achieves this through the port scanning of every device broadcasting to the open internet. We can find devices in Shodan based on their IP address, an IP address is like the mailing address of a computer or any internet connected device. We can send information to a device and receive information from a device by talking to its IP. Every device on Shodan will have open ports, a port is basically a note that is connected to the IP address to tell the device where your message should go once it is received. There are ports for emails, webpages, cameras, and remote connections. The most common ports used can be found here:

[https://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers). The type of port you find is going to determine what you are going to see! Lastly, let's go over the idea of pings. A ping request basically asks the device if it's alive. If it is alive it will respond, there is a time attached to these responses, this is how long it took for the device to respond. If the device is dead or purposely not responding to pings, the request will time out, this is how Shodan finds working devices to probe for open ports.

```
(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=50.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=52.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=47.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=47.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=49.7 ms
^C File system
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4037ms
rtt min/avg/max/mdev = 47.602/49.665/52.728/1.933 ms
```

Successful ping request

```
(kali㉿kali)-[~]
$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
From 192.168.1.50 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.1.200 ping statistics ---
115 packets transmitted, 0 received, +1 errors, 100% packet loss, time 116726ms
```

Failed ping request

## USING FILTERS

Shodan uses tools known as filters. These filters allow you to narrow down your results based on what you are trying to find. Instead of searching through millions of devices, you can choose to search just for devices that meet your criteria. This could include searching for devices in your town, those who are running services on a specific port, or even showing just webcams! This can be very useful as if you are trying to find multiple servers that are running a program on port 754 you can have all your results neatly organized without ever having to ping the device yourself. The full list of filters can be found here: <https://www.shodan.io/search/filters> with a cheatsheet of the most common filters below.

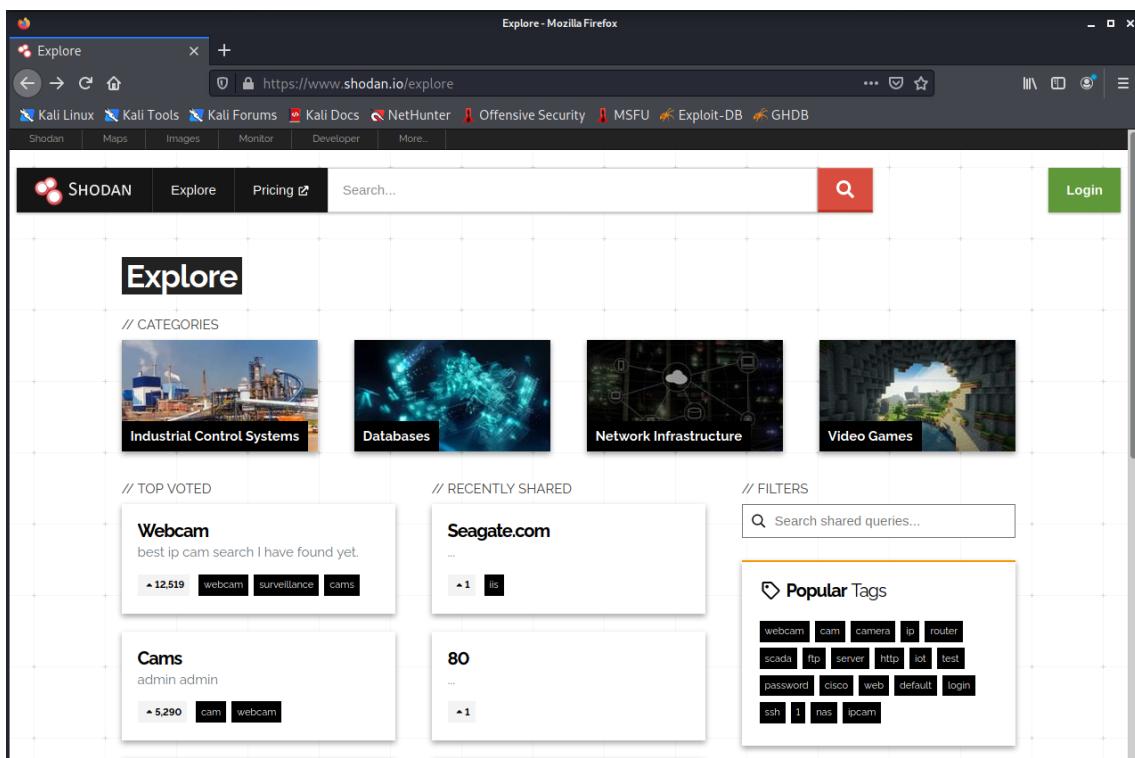
### Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
<code>city</code>	Name of the city	Devices in San Diego
<code>country</code>	2-letter Country code	Open ports in the United States
<code>http.title</code>	Title of the website	"Hacked" Websites
<code>net</code>	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255
<code>org</code>	Name of the organization that owns the IP space	Devices at Google
<code>port</code>	Port number for the service that is running	SSH servers
<code>product</code>	Name of the software that is powering the service	Samsung Smart TVs
<code>screenshot.label</code>	Label that describes the content of the image	Screenshots of Industrial Control Systems
<code>state</code>	U.S. State	Devices in Texas

## HOW TO USE SHODAN

In order to access Shodan, first go to <https://www.shodan.io/explore> in order to view the homepage of the site. Here you can see all of the most popular categories that people use to view devices. On the top search bar you can manually enter a search item such as an ip or filter combo. Located on the column to the right of the screen are popular tags that can be used to quickly search and find devices.



However, before we can start searching the internet for all it has to offer, we have to make an account. We can create one at: <https://account.shodan.io/login>. Once we have made an account, we can return to the explore page and start searching!

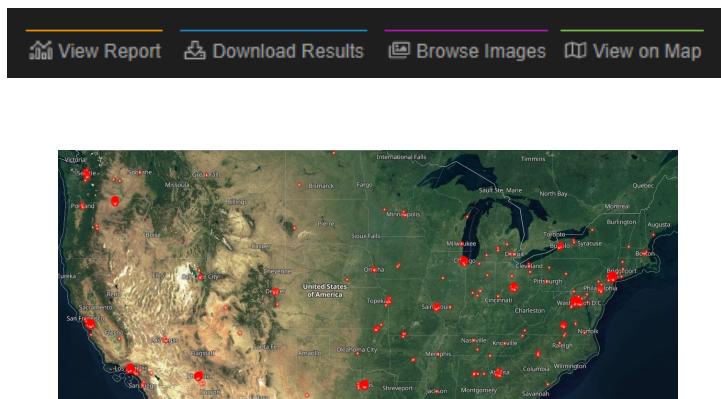
## VIEWING REMOTE DESKTOP

Remote desktop is a tool that allows you to connect to your computer over the internet. This is very useful for accessing your devices from a different location but if left unsecure your

machine can be found and accessed by anyone who scans your IP address. You can search for this by using the filter “**port:3389 has\_screenshot:true**”. Port 3389 is the port dedicated to remote desktop, you can also filter by country adding “**country:US**” to your filter (use the 2 digit country code). You should find a ton of desktops with this enabled and you can see the users who have accounts on these machines.



On the top bar of the search results screen, you can click “**Browse Images**” to see a screen view of all the vulnerable devices, or you can click “**View on Map**” to see where these machines are physically located, you can move and zoom the map, then click the pin to see information about that device.



## VIEWING WEBCAMS

One of the most controversial uses of Shodan is the ability to view others webcams. We are able to achieve this by searching different webcam services available on the open internet.

For this demonstration we are going to be viewing devices that are currently running the service, “webcamxp”. WebcamXP is an outdated webcam and network camera software for legacy Windows devices that allows its users to view the webcam remotely. Similar to other aspects in the technology industry, even though it's outdated and insecure, people still use the service because of compatibility issues or more commonly, laziness.

We can view these devices by going to the search bar on the explore page and using the keyword “**webcamxp**” hit enter. Once we've done this we can start to scroll through the different devices running this service (Seen Below). Spend a few minutes searching through these devices and formulate what security issues could come from this.

**TOTAL RESULTS** ..... **464**

**TOP COUNTRIES**



Russian Federation	90
United States	56
Germany	35
Italy	31
Ukraine	31
<a href="#">More...</a>	

**TOP PORTS**

8080	153
80	32
8081	21
81	18
52869	16
<a href="#">More...</a>	

**TOP ORGANIZATIONS**

Softline Trade JSC	68
PJSC Ukrtelecom	26

**View Report** **Download Results** **Browse Images** **View on Map**

**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**webcamXP 5** 

89.242.21.39  
host-89-242-21-39.  
as13285.net  
Opal Telecom DSL  
United Kingdom, Glasgow

HTTP/1.1 200 OK  
Connection: close  
Content-Type: text/html; charset=utf-8  
Content-Length: 7360  
Cache-control: no-cache, must revalidate  
Date: Fri, 24 Sep 2021 15:01:07 GMT  
Expires: Fri, 24 Sep 2021 15:01:07 GMT  
Pragma: no-cache  
Server: webcamXP 5

2021-09-24T15:01:06.983369



**webcamXP 5**

```

95.248.81.168   HTTP/1.1 200 OK
host:95.248.81.168   Connection: close
8.retail.telecomitali
a.it   Content-Type: text/html; charset=utf-8
Telecom Italia   Content-Length: 7589
S.p.A.   Cache-control: no-cache, must revalidate
Italy, Florence   Date: Fri, 24 Sep 2021 14:51:50 GMT
   Expires: Fri, 24 Sep 2021 14:51:50 GMT
Pragma: no-cache
Server: webcamXP 5

```

2021-09-24T14:52:01.357034

**93.90.222.25**

```

Softline Trade JSC   HTTP/1.1 200 OK
 Russian   Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDAT S.A., AIOWS/1.00,
Federation, Moscow


```

**honeypot****webcamXP 5**

```

64.118.101.66   HTTP/1.1 200 OK
64.118.101.66.static.   Connection: close
stl.net   Content-Type: text/html; charset=utf-8
Sierra Tel Internet   Content-Length: 7413
 United   Cache-control: no-cache, must revalidate
States, Oakhurst   Date: Fri, 24 Sep 2021 14:23:09 GMT
   Expires: Fri, 24 Sep 2021 14:23:09 GMT
Pragma: no-cache
Server: webcamXP 5

```

2021-09-24T14:23:14.422188



## VIEWING GAME SERVERS

You can also use Shodan to look at video game servers! Click on the explore tab and click on the Video Games category. You'll see several games such as Minecraft, Counter Strike, and Rust. In this lab, we'll be taking a look at Minecraft servers. **Click on Video Games, then Explore Minecraft** to see how many servers you can find on Shodan. You will be able to see the version, a description of the server, the number of online players, and the maximum number of players. You can also see the server IP address as well as the location where the server is being hosted. Click around on the IP addresses to see a more detailed view of the servers. You can see what ports are being used, the domains being used to host the servers, and in some cases it will show potential vulnerabilities. Take a few minutes to click around on different servers and see if you can find any with vulnerabilities that Shodan suspects.

SHODAN
Explore
Downloads
Pricing
product:minecraft

Account

TOTAL RESULTS: 182,066

TOP COUNTRIES:

Country	Count
United States	62,977
Germany	34,372
Canada	11,145
Japan	10,880
France	9,133
More...	

TOP PORTS:

Port	Count
25565	182,039
8001	3
9999	3
2001	2
5001	2
More...	

TOP ORGANIZATIONS:

Organization	Count
CLOUDS	49,000

**157.90.154.40**

static.40.154.90.157.clients.your-server.de  
Hetzner Online GmbH  
Germany, Oberdorla

**videogame**

Minecraft Server:  
Version: Spigot 1.17 (Protocol 755)  
Description: A Minecraft Server  
Online Players: 0  
Maximum Players: 20

**158.62.200.92**

158.62.200.92.static.bisecthosting.com  
BisectHosting  
United States, Dallas

**videogame**

Minecraft Server:  
Version: 1.17.1 (Protocol 756)  
Description: Better Minecraft [FABRIC]  
Online Players: 0  
Maximum Players: 40

## EXERCISES:

### 1: Location Discovery:

For this exercise, try finding open devices within your hometown! Shodan's filters allow you to discover devices in an area. Below is a list of devices in Detroit, MI

The screenshot shows the Shodan search interface with the following details:

- TOTAL RESULTS:** 587,493
- TOP PORTS:**

Port	Count
443	59,683
80	58,474
53	33,452
2087	30,059
21	28,417
- TOP ORGANIZATIONS:**

Organization	Count
A2 Hosting, Inc.	369,727
Precipice	37,858
SoftwareWorks Group, Inc.	30,938
Liquid Web, L.L.C	21,857
Comcast Cable Communications, Inc.	12,603
- TOP PRODUCTS:**

Product	Count
Exim smtpd	56,298
Apache httpd	50,638
Pure-FTPd	24,733
MySQL	21,606
nginx	15,555
- Result Details for US Sports Camps - NIKE Sports Camps:**
  - SSL Certificate:**
    - Issued By: DigiCert EV RSA CA 2018
    - Issued To: ussportscamps.com
    - Supported SSL Versions: TLSv1.2
  - HTTP Headers:**

```
HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 16:54:17 GMT
Server: Apache
X-Powered-By: Craft CMS
X-Hostname: mce825-nodel.nexcess.net
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```
- Result Details for 307 Temporary Redirect:**
  - SSL Certificate:**
    - Issued By: DigiCert TLS RSA SHA256 2020 CA1
    - Issued To: \*wayne.edu
    - Supported SSL Versions: TLSv1.2, TLSv1.3
  - HTTP Headers:**

```
HTTP/1.1 307 Temporary Redirect
Server: nginx/1.20.1
Date: Fri, 24 Sep 2021 16:52:33 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 231
Connection: keep-alive
Location: http://sis.wayne.edu/
```

### 2: Find legacy hardware based on operating systems:

Oftentimes people are lazy or don't have the ability to upgrade old computer systems that are highly insecure. In this exercise, try to find devices that are still running Windows XP which ended security support on January 14, 2020! Below is a list of computers running Raspbian

**TOTAL RESULTS**

**72,558**

**TOP COUNTRIES**

Country	Results
Germany	9,217
United States	8,213
France	5,220
Korea, Republic of	4,737
Italy	4,231

[More...](#)

**84.113.250.210**

84-113-250-210.cable.dynamic.surfer.at  
UPC Austria  
Austria, Vienna

SSH-2.0-OpenSSH\_7.9p1 Raspbian-10+deb10u2  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAAQDQ8QkQw+D2fA9QhkK3hF1DcsVLt5vHBm7e12amNz3Gn9xc7RpuVLwAfYvuME73spH1zCDYecNmShzEVd7MgRku/LnzqjY2/UxkJ16Si385tIWChOCxQEyW11CQhhZ1zQ1PUtBQ8pXik1StcHnBp3K7en1737FQa+K4yB10XKTBoAySaNtYJ83m8XH0W394N2rykRmW...

**92.64.158.89**

92-64-158-89.biz.kpn.net  
Men VI  
Netherlands, Amsterdam

SSH-2.0-OpenSSH\_7.9p1 Raspbian-10+deb10u2  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAAQDDE9rqxnFM2YHH9zXdiVI+EqvR8sjBbfx1c/N3zKOFIDFV1tnfNg/VJjn2zf1PhUhe dinOns1qNyJS9hD1dbmmdJ9C6HX2TjG+u834U9asqjinX/4JSVa9RMKhfyyeM65EpjPu/QOAnaAnOUF3JG6/HwhX7mGT06dXK1dBiMnvbnypU4nD5REQMjV3knYH529Gpk/dw...

**87.150.44.52**

p57962c34.dip0.t-ipconnect.de  
Deutsche Telekom AG  
Germany, Wandlitz

SSH-2.0-OpenSSH\_6.7p1 Raspbian-6+deb8u3  
Key type: ssh-rsa  
Key: AAAAB3NzaC1yc2EAAAQABAAAQDNmrsv34yEyCCQylukRbfplaeKuKEa6Qrv9nZm5ycq/OGFVmK3+mxnfF+urt+P+wZGSWa4ymUcFL4Rbmz1/JY7WTW5DmHEqzAcyHnIDObqc510c37RQGshtrE62svlQE06Co04+Njg6Budtech1f4xWdPprzB3uP5NBgCveZgKw8Qn6icWtBY7wDqDIixFimDtKfuQrk...

**90.39.71.188**

## REVIEW

1: Web servers are hosted on what ports?

- A) 89/314
- B) 312/765
- C) 80/443
- D) 14/214

2: Default security settings are often enough  
to be secure on the internet (True/False)

3: Which isn't a filter on shodan?

- A) city
- B) webcam
- C) jonstar
- D) product:minecraft

4: Shodan is used *only* for hacking it has no  
purpose for securing your network  
(True/False)

5: Port scanning your network allows what?

- A) See services that face the open internet
- B) Detect malicious/unknown servers
- C) Know your networks vulnerabilities
- D) All of the above

6: Select the correct statement

- A) Using Shodan is Illegal and accessing  
devices is legal
- B) Using Shodan is legal and accessing  
devices is illegal
- C) Using Shodan is Illegal and accessing  
devices is illegal
- D) Using Shodan is legal and accessing  
devices is legal

Answers: 1:C 2:F 3:C 4:F 5:D 6:B